UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,713	11/27/2000	Jae-han Park	Q61823	4060

7590   01/27/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3202

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 14 have been presented for examination. Claim 7 has been

amended in an amendment filed 10/12/2004. Claims 1 – 14 have been examined.

Response to Arguments

2.   Applicant's arguments with respect to the subject matter of the instant

claims have been fully considered but are not persuasive.

3.   As per claim 1, Applicant asserts "Bluetooth fail to teach or suggest that a

predetermined message is sent according to a current operation mode and is

stored when an authentication-response message to the first authentication-

request message is received". However, Examiner is interpreting, in Bluetooth,

when the authentication is finished the link key must be created (Bluetooth: see for

example, Part-C Section 3.3.4 1st Sentence) and subsequently the link key

message is sent and the response message is received (Bluetooth: see for

example, Part-C Section 3.3.4 Figure/Sequence 7). The selection of the link key,

either LMP_unit_key or LMP_comb_key, is determined based on whether

response message received matches the message being sent or not – or more

specifically, based on which message being sent and which message being

received (between LMP_unit_key message and LMP_comb_key message)

(Bluetooth: see for example, Part-C Section 3.3.4, Page 198, Bullets 1 – 3).

Thereby, Examiner notes the predetermined message being sent is interpreted as

the "key selection message" as addressed above and this predetermined message

"must" be stored (inherently) so that the decision rule for key selection can be

applied to compare the message being sent against the message being received /

responded (Bluetooth: see for example, Part-C Section 3.3.4 Line 9 – 13, Page

198, Bullets 1 – 3).

4.   As per claim 7, Applicant remarks "Shona fails to teach after performing the

step (a) and prior to performing the step (c), checking of an authentication

condition of the present device is performed". Examiner notes "checking of an

authentication condition" can be interpreted into two elements: (I) when to check

the authentication condition and (II) how to determine the authentication condition.

Bluetooth is relied upon for providing a mechanism regarding (I) when to check the

authentication condition – i.e., after performing the step (a) sending a response

message corresponding to a first authentication request message when the first

authentication-request message from another device that wants to establish a

connection is received (Bluetooth: see for example, PART C, Section 3.2

Authentication and Section 3.3.1 & Section 3.3.2, Sequence 3 / 4) (Bluetooth: see

for example, Part-C Section 3.3 Figure/Sequence 3 / 4) and prior to performing the

step (c) storing the predetermined message and sending a second

authentication-request message to the other device when the result of checking

indicates that a mutual authentication is required (Bluetooth: see for example,

PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154 & Figure 14.11

and PART B, Section 14.4 Authentication 4th Paragraph, page 170 & PART C,

Section 3.3, Sequence 4. Regarding (II) how to determine the authentication

condition, Bluetooth only discloses Link Manager coordinates the indicated
authentication preference (i.e. checking of an authentication condition – mutual
authentication required or not) (Bluetooth: see for example, Part-B Section 14.4,
3rd Paragraph Page. 170). However, Bluetooth does not disclose expressly how to
determine the authentication condition. In need of this, Shona is merely relied
upon that the indication / determination of mutual authentication (instead of
unilateral authentication) required can be simply based on a flag setting = "10"
(Shona: see for example, Column 5 Line 61 – 67).

5.   As per claim 12, Applicant remarks "Shona fails to teach a determination, of
whether an authentication procedure will be performed as a unilateral
authentication procedure or a mutual authentication procedure, is made according
to an authentication condition". See the same response to argument for claim 7
addressed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for
all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the
> prior art are such that the subject matter as a whole would have been obvious at the time the invention
> was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability
> shall not be negatived by the manner in which the invention was made.

6.   Claims 1 – 6, 8 – 10 and 13 are rejected under 35 U.S.C. under 35 U.S.C.

103(a) as being unpatentable over Bluetooth (Specification of the Bluetooth

System Version 1.0 A, July 26th 1999), hereinafter referred to as Bluetooth.

7.   As per claim 1, Bluetooth teaches an authentication method for establishing

a connection between devices that can wirelessly communicate data, the method

comprising the steps of:

a.   sending a first authentication-request message to another device to perform

an authentication procedure with the other device to which a connection is wanted

(Bluetooth: see for example, PART B, Section 3.2 Authentication page 194 and

Section 3.3 Pairing page 196);

b.   ·sending a predetermined message according to a current operation mode

to the other device and storing the predetermined message when an

authentication-response message to the first authentication-request message is

received (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link

Key, page 197: when the authentication is finished the link key must be created

(Bluetooth: see for example, Part-C Section 3.3.4 1st Sentence) and subsequently

the link key message is sent and the response message is received (Bluetooth:

see for example, Part-C Section 3.3.4 Figure/Sequence 7). The selection of the

link key, either LMP_unit_key or LMP_comb_key, is determined based on whether

response message received matches the message being sent or not – or more

specifically, based on which message being sent and which message being

received (between LMP_unit_key message and LMP_comb_key message)

(Bluetooth: see for example, Part-C Section 3.3.4, Page 198, Bullets 1 – 3).

Thereby, Examiner notes the predetermined message being sent is interpreted as

the "key selection message" as addressed above and this predetermined message

"must" be stored (inherently) so that the decision rule for key selection can be

applied to compare the message being sent against the message being received /

responded (Bluetooth: see for example, Part-C Section 3.3.4 Line 9 – 13, Page

198, Bullets 1 – 3).

Bluetooth does not expressly teach:

c.   after performing the step (b), checking whether a received first message is

a response message corresponding to the predetermined message when the first

message from the other device is received;

8.   However, it would have been obvious to a person of ordinary skill in the art

at the time the invention was made to modify the Bluetooth specification in an

explicit way to accommodate, for the originator (or the verifier), checking whether a

received first message is a response message corresponding to the

predetermined message when the first message from the other device is received

because (a) Bluetooth teaches mutual authentication is achieved by performing

first the authentication procedure in one direction and, if successful, immediately

followed by performing the authentication procedure in the reversed direction

(Bluetooth: see for example, PART B, Section 14.2.2.2 Authentication 2nd

Paragraph, page 154), and (b) Bluetooth further teaches the application should

indicate who has to be authenticated by whom. Certain applications only require a

one-way authentication. However, in some peer-to-peer communications, one

might prefer a mutual authentication in which each unit is subsequently the

challenger (verifier) in two authentication procedures and thus the mutual

authentication is indeed an option during the authentication procedure (Bluetooth:

see for example, Figure 14.11 and PART B, Section 14.4 Authentication 4th

Paragraph, page 170). Therefore, based upon the authentication condition (either

unilateral-authentication or mutual-authentication or), the response message could

be either the link key selection message (Bluetooth: see for example, PART C,

Section 3.3.4) or the start of the reverse authentication from the other side of

device (Bluetooth: see for example, PART B, Section 14.4 Page 170 Line 6 – 10).

d.   sending a response message corresponding to a second

authentication-request message to the other device when the result of checking in

the step (c) indicates that the first message is the second authentication request

message (Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4

Authentication 4th Paragraph, page 170, Line 7 – 11);

e.   after performing the step (d), checking whether a second message is a

response message corresponding to the predetermined message when the

second message from the other device is received (Bluetooth: see for example,

PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 8 & Bullets 1 – 3); and

f.   finishing the authentication procedure when the result of checking in the

step (e) indicates that the second message is a response message corresponding

to the predetermined message (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 9 – 16 & Bullets 1 – 3).

9.   As per claim 2 and 6, Bluetooth teaches the claimed invention as described above (see claim 1 and 4 respectively). Bluetooth as modified further teaches in the step (b), when the current operation mode is a pairing process, a message for generating a link key is sent as the predetermined message and stored (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16), and when the current operation mode is not a pairing process, a message of connection-establishment-completion is sent as the predetermined message and stored (Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd Paragraph); and the step (f) further comprises the sub-steps of:

(f1)   generating a link key before finishing the authentication procedure when the current operation mode is a pairing process (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16); and

(f2)   finishing the authentication procedure and establishing a connection to the other device when the current operation mode is not a pairing process (Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd Paragraph and Figure 4.1).

10.   As per claim 3, Bluetooth teaches the claimed invention as described above (see claim 1). Bluetooth as modified further teaches the step (b) further comprises the sub-steps of:

(b1)   checking whether the authentication-response message is valid using key

information and random information (Bluetooth: see for example, PART C, Section

3.2 Authentication and Section 3.2.1); and

(b2)   processing an authentication failure when the result of checking in the step

(bl) indicates that the authentication-response message is not valid (Bluetooth: see

for example, PART C, Section 3.2.1).

11.   As per claim 4, Bluetooth teaches the claimed invention as described above

(see claim 3). Bluetooth as modified further teaches in the step (b l), the key

information is held by the present device and the random information was used in

sending the first authentication message (Bluetooth: see for example, PART C,

Section 3.2 Authentication).

12.   As per claim 5, Bluetooth teaches the claimed invention as described above

(see claim 1). Bluetooth as modified further teaches (g) finishing the

authentication procedure when the result of checking in the step (c) indicates that

the received first message is a response message corresponding to the

predetermined message (Bluetooth: see for example, PART C, Section 4

Connection Establishment, 3rd Paragraph and Figure 4.1).

13.   As per claim 8, Bluetooth teaches the claimed invention as described above

(see claim 6). Bluetooth as modified further teaches in the step (d), when the

predetermined message received in the step (b) is a message for generating a link

key, the present device sends a response message corresponding to the message

for generating a link key to the other device, generates a link key, and then

finishes the authentication procedure (Bluetooth: see for example, PART C,

Section 3.3.4 Creation of the Link Key, Line 6 – 16 and Sequence 7); and when

the predetermined message received in the step (b) is a message of

connection-establishment-completion, the present device sends a response

message corresponding to the message of connection-establishment completion

to the other device, finishes the authentication procedure, and then establishes a

connection to the other device (Bluetooth: see for example, PART C, Section 4

Connection Establishment, 3rd Paragraph and Figure 4.1).

14.   As per claim 9, Bluetooth teaches the claimed invention as described above
(see claim 6). Bluetooth as modified further teaches the step (d) further comprises
the sub-steps of:

(d1)   checking whether the response message corresponding to the second

authentication-request message is valid when the response message

corresponding to the second authentication-request message is received by using

random information and key information (Bluetooth: see for example, Figure 14.11

and PART B, Section 14.4 Authentication 4th Paragraph, page 170); and

(d2)   processing an authentication failure when the result of checking in the step

(dl) indicates that the response message is not valid (Bluetooth: see for example,

PART C, Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

15.   As per claim 10, Bluetooth teaches the claimed invention as described

above (see claim 9). Bluetooth as modified further teaches in the step (dl), the

present device holds the key information and the random information was used in

sending the first authentication message (Bluetooth: see for example, PART C,

Section 3.2 Authentication).

16.   As per claim 13, Bluetooth teaches the claimed invention as described

above (see claim 10). Bluetooth as modified further teaches performing the

authentication procedure, when the authentication condition of the device that

receives the authentication request is set to require the mutual authentication

procedure, the mutual authentication procedure is performed by sending an

authentication request message to the device that requests an authentication

(Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4

Authentication 4th Paragraph, page 170).

17.   Claims 7, 11, 12 and 14 are rejected under 35 U.S.C. under 35 U.S.C.

103(a) as being unpatentable over Bluetooth (Specification of the Bluetooth

System Version 1.0 A, July 26th 1999), hereinafter referred to as Bluetooth, in view

of Shona (Patent Number: 5799085), hereinafter referred to as Shona.

18.   As per claim 7, Bluetooth teaches an authentication method for establishing

a connection between devices that can wirelessly communicate data, the method

comprising the steps of:

a.   sending a response message corresponding to a first authentication

request message when the first authentication-request message from another

device that wants to establish a connection is received (Bluetooth: see for

example, PART C, Section 3.2 Authentication and Section 3.3.1 & Section 3.3.2,

Sequence 3 / 4);

b.   Bluetooth does not expressly (and completely) teach, after performing the

step (a), checking an authentication condition of the present device when a

predetermined message from the other device is received. Examiner notes this is

because "checking of an authentication condition" can be interpreted into two

elements: (I) when to check the authentication condition and (II) how to determine

the authentication condition. Bluetooth discloses providing a mechanism regarding

(I) when to check the authentication condition – i.e., after performing the step (a)

sending a response message corresponding to a first authentication request

message when the first authentication-request message from another device that

wants to establish a connection is received (Bluetooth: see for example, PART C,

Section 3.2 Authentication and Section 3.3.1 & Section 3.3.2, Sequence 3 / 4)

(Bluetooth: see for example, Part-C Section 3.3 Figure/Sequence 3 / 4) and prior

to performing the step (c) storing the predetermined message and sending a

second authentication-request message to the other device when the result of

checking indicates that a mutual authentication is required (Bluetooth: see for

example, PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154 &

Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170 &

PART C, Section 3.3, Sequence 4. Regarding (II) how to determine the

authentication condition, Bluetooth only discloses Link Manager coordinates the

indicated authentication preference (i.e. checking of an authentication condition –

mutual authentication required or not) (Bluetooth: see for example, Part-B Section

14.4, 3rd Paragraph Page. 170). However, Bluetooth does not disclose expressly

how to determine the authentication condition.

19.   Shona teaches how to determine an authentication condition of the present

device when a predetermined message from the other device is received (Shona:

see for example, Column 5 Line 61 – 67: Shona teaches the indication /

determination of mutual authentication (instead of unilateral authentication)

required can be simply based on a flag setting = "10").

20.   Therefore, it would have been obvious to a person of ordinary skill in the art

at the time the invention was made to combine the teaching of Shona within the

system of Bluetooth as modified because (a) Bluetooth teaches mutual

authentication is achieved by performing first the authentication procedure in one

direction and, if successful, immediately followed by performing the authentication

procedure in the reversed direction (Bluetooth: see for example, PART B, Section

14.2.2.2 Authentication 2nd Paragraph, page 154), and (b) Bluetooth further

teaches the application should indicate who has to be authenticated by whom.

Certain applications only require a one-way authentication. However, in some

peer-to-peer communications, one might prefer a mutual authentication in which

each unit is subsequently the challenger (verifier) in two authentication procedures

and thus the mutual authentication is indeed an option during the authentication

procedure (Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4

Authentication 4th Paragraph, page 170), and (c) Shona teaches a method of

effecting mutual authentication between two entities that the authentication

condition is determined by the setting of an mutual authentication enabling flag

(Shona: see for example, Column 5 Line 61 – 67).

21.   Bluetooth as modified further teaches:

c.   after performing the step (b), storing the predetermined message and

sending a second authentication-request message to the other device when the

result of checking indicates that a mutual authentication is required (Bluetooth: see

for example, PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154 &

Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170 &

PART C, Section 3.3, Sequence 4. Regarding "storing the predetermined

message", see addressed above).

d.   after performing the step (c), sending a response message corresponding

to the message stored in the step (c) to the other device when a response

message from the other device corresponding to the second

authentication-request message is received, and finishing the authentication

procedure (Bluetooth: see for example, PART C, Section 4 Connection

Establishment,3rd Paragraph and Figure 4.1).

22.   As per claim 12, Bluetooth teaches determining whether an authentication

procedure for establishing a connection between devices that want to

communicate data is performed as a unilateral authentication procedure or as a

mutual authentication procedure (Bluetooth: see for example, PART B, Section

14.2.2.2 Authentication 2nd Paragraph, page 154 & Figure 14.11 and PART B,

Section 14.4 Authentication 4th Paragraph, page 170). However, Bluetooth does

not expressly teach this decision is determined according to an authentication

condition which enables receiving an authentication request in the two devices that

can communicate data; and performing the authentication procedure.

Examiner notes this is because "decision is determined according to an

authentication condition" can be interpreted into two elements: (I) when to check

the authentication condition and (II) how to determine the authentication condition.

Bluetooth discloses providing a mechanism regarding (I) when to check the

authentication condition – i.e., after performing the step (a) sending a response

message corresponding to a first authentication request message when the first

authentication-request message from another device that wants to establish a

connection is received (Bluetooth: see for example, PART C, Section 3.2

Authentication and Section 3.3.1 & Section 3.3.2, Sequence 3 / 4) (Bluetooth: see

for example, Part-C Section 3.3 Figure/Sequence 3 / 4) and prior to performing the

step (c) storing the predetermined message and sending a second

authentication-request message to the other device when the result of checking

indicates that a mutual authentication is required (Bluetooth: see for example,

PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154 & Figure 14.11

and PART B, Section 14.4 Authentication 4th Paragraph, page 170 & PART C,

Section 3.3, Sequence 4. Regarding (II) how to determine the authentication

condition, Bluetooth only discloses Link Manager coordinates the indicated

authentication preference (i.e. checking of an authentication condition – mutual

authentication required or not) (Bluetooth: see for example, Part-B Section 14.4,

3rd Paragraph Page. 170). However, Bluetooth does not disclose expressly how to

determine the authentication condition.

23.   Shona teaches how to determine an authentication condition of the present

device when a predetermined message from the other device is received (Shona:

see for example, Column 5 Line 61 – 67: Shona teaches the indication /

determination of mutual authentication (instead of unilateral authentication)

required can be simply based on a flag setting = "10").

24.   Therefore, it would have been obvious to a person of ordinary skill in the art

at the time the invention was made to combine the teaching of Shona within the

system of Bluetooth as modified because (a) Bluetooth teaches mutual

authentication is achieved by performing first the authentication procedure in one

direction and, if successful, immediately followed by performing the authentication

procedure in the reversed direction (Bluetooth: see for example, PART B, Section

14.2.2.2 Authentication 2nd Paragraph, page 154), and (b) Bluetooth further

teaches the application should indicate who has to be authenticated by whom.

Certain applications only require a one-way authentication. However, in some

peer-to-peer communications, one might prefer a mutual authentication in which

each unit is subsequently the challenger (verifier) in two authentication procedures

and thus the mutual authentication is indeed an option during the authentication

procedure (Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4

Authentication 4th Paragraph, page 170), and (c) Shona teaches a method of effecting mutual authentication between two entities that the authentication condition is determined by the setting of an mutual authentication enabling flag (Shona: see for example, Column 5 Line 61 – 67: Shona teaches the indication / determination of mutual authentication (instead of unilateral authentication) required can be simply based on a flag setting = "10").

25.   As per claim 11 and 14, Bluetooth teaches the claimed invention as described above (see claim 6 and 10 respectively). Bluetooth as modified does not expressly teach in the step (b) authentication enable information is checked as the authentication condition.

26.   Shona further teaches in the step (b) authentication enable information is checked as the authentication condition (Shona: see for example, Column 5 Line 61 – 67: An mutual authentication flag is set to enable the mutual authentication function between two entities).

27.   Same rationale of combination applies herein as above in rejecting Claim 12.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of

time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire

THREE MONTHS from the mailing date of this action. In the event a first reply is

filed within TWO MONTHS of the mailing date of this final action and the advisory

action is not mailed until after the end of the THREE-MONTH shortened statutory

period, then the shortened statutory period will expire on the date the advisory

action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing date
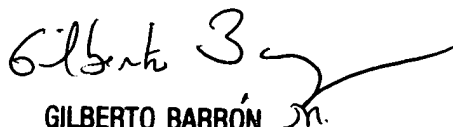
of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100